Document made available under the Patent Cooperation Treaty (PCT)

International application number: PCT/SE04/001735

International filing date: 24 November 2004 (24.11.2004)

Document type: Certified copy of priority document

Document details: Country/Office: US
Number: 60/551,040
Filing date: 09 March 2004 (09.03.2004)

Date of receipt at the International Bureau: 10 January 2005 (10.01.2005)

Remark: Priority document submitted or transmitted to the International Bureau in compliance with Rule 17.1(a) or (b)

World Intellectual Property Organization (WIPO) - Geneva, Switzerland
Organisation Mondiale de la Propriété Intellectuelle (OMPI) - Genève, Suisse

PCT / SE 2004 / 0 0 1 7 3 5
17-12-2004

PA 1255259

THE UNITED STATES OF AMERICA

TO ALL TO WHOM THESE PRESENTS SHALL COME:

UNITED STATES DEPARTMENT OF COMMERCE

United States Patent and Trademark Office

December 03, 2004

THIS IS TO CERTIFY THAT ANNEXED HERETO IS A TRUE COPY FROM THE RECORDS OF THE UNITED STATES PATENT AND TRADEMARK OFFICE OF THOSE PAPERS OF THE BELOW IDENTIFIED PATENT APPLICATION THAT MET THE REQUIREMENTS TO BE GRANTED A FILING DATE UNDER 35 USC 111.

APPLICATION NUMBER: *60/551,040*
FILING DATE: *March 09, 2004*

By Authority of the
COMMISSIONER OF PATENTS AND TRADEMARKS

H. L. Jackson

H. L. JACKSON
Certifying Officer

13281 U.S.PTO

Mail Stop Provisional Patent Application

PTO/SB/16 (6-95)
Approved for use through 04/11/98. OMB 0651-0037
Patent and Trademark Office, U.S. DEPARTMENT OF COMMERCE

PROVISIONAL APPLICATION COVER SHEET

This is a request for filing a PROVISIONAL APPLICATION under 37 CFR 1.53 (c).

	Docket Number	4147-67	Type a plus sign (+) inside this box→	+

INVENTOR(S)/APPLICANT(S)

LAST NAME	FIRST NAME	MIDDLE INITIAL	RESIDENCE (CITY AND EITHER STATE OR FOREIGN COUNTRY)
OYAMA	Johnson		Tokyo, Japan
KATO	Ryoji		Yokusuka Kanagawa, Japan

15535 U.S. PTO 60/551040 030904

TITLE OF THE INVENTION (280 characters)

ACCESS CONTROL IN MOBILE NETWORKS

CORRESPONDENCE ADDRESS

Direct all correspondence to:

☒ **Customer Number:** **23117**

Type Customer Number here

Place Customer Number Bar Label Here →

ENCLOSED APPLICATION PARTS *(check all that apply)*

☒ Specification — Number of Pages: 8

☒ Drawing(s) — Number of Sheets: 5

☐ Applicant claims "small entity" status.
☐ "Small entity" statement attached.

☐ Other (specify)

METHOD OF PAYMENT *(check one)*

☒ A check or money order is enclosed to cover the Provisional filing fees ($160.00)/($80.00)

☒ The Commissioner is hereby authorized to charge any deficiency, or credit any overpayment, in the fee(s) filed, or asserted to be filed, or which should have been filed herewith (or with any paper hereafter filed in this application by this firm) to our Account No. 14-1140. A duplicate copy of this sheet is attached.

PROVISIONAL FILING FEE AMOUNT ($): 160.00

The invention was made by an agency of the United States Government or under a contact with an agency of the United States Government.

☒ No.

☐ Yes, the name of the U.S. Government agency and the Government contract number are:

Respectfully submitted,

SIGNATURE [signature] DATE March 9, 2004

TYPED or PRINTED NAME H. Warren Burnam, Jr.

REGISTRATION NO. *(if appropriate)* 29,366

☐ Additional inventors are being named on separately numbered sheets attached hereto.

PROVISIONAL APPLICATION FILING ONLY

Burden Hour Statement: This form is estimated to take .2 hours to complete. Time will vary depending upon the needs of the individual case. Any comments on the amount of time you are required to complete this form should be sent to the Mail Stop Comments - Patents, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450, and to the Office of Information and Regulatory Affairs, Office of Management and Budget (Project 0651-0037), Washington, DC 20503. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Mail Stop Provisional Patent Application, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

824678

Atty. Dkt. 4147-67
PE19317US00

U.S. PROVISIONAL PATENT APPLICATION

Inventor(s): Johnson OYAMA
Ryoji KATO

Invention: ACCESS CONTROL IN MOBILE NETWORKS

NIXON & VANDERHYE P.C.
ATTORNEYS AT LAW
1100 NORTH GLEBE ROAD, 8TH FLOOR
ARLINGTON, VIRGINIA 22201-4714
(703) 816-4000
Facsimile (703) 816-4100

824679

ACCESS CONTROL IN MOBILE NETWORKS

TECHNICAL FIELD OF THE INVENTION

The present invention generally relates to access control in communication networks, and in particular to access control in mobile networks.

BACKGROUND OF THE INVENTION

Access control is generally applicable to network nodes in communication networks such as mobile networks, and more specifically NEMO-based (Network Mobility) mobile networks, HIP-based (Host Identity Protocol) mobile networks or mobile networks based on prefix scope binding update.

For example, the Network Mobility (NEMO) Basic Protocol described in reference [1] enables mobile networks to attach to different points in the Internet. The protocol is an extension of Mobile IPv6 and allows for session continuity for every node in the mobile network as the network moves. It also allows every node in the mobile network to be reachable while moving around. The Mobile Router, which connects the network to the Internet, runs the NEMO Basic Support protocol with its Home Agent. The protocol is designed in such a way that network mobility is transparent to the nodes inside the mobile network.

Reference [2] describes a basic AAA (Authentication, Authorization, and Accounting) model for NEMO, as well as various usage scenarios. Regarding client access authentication for nodes in NEMO-based Mobile Networks, the draft proposes a AAA solution between Visiting Mobile Node and Mobile Router which essentially has the Mobile Router performing/behaving as a Network Access Server. The Visiting Mobile Node will first initiate an access request by sending relevant messages to the Mobile Router it attached to using a "link-local" AAA protocol. The Mobile Router contacts

an external AAA server (e.g., in the Visiting Mobile Node's home network) to perform the actual authentication and authorization by employing one of the "global" AAA protocols. However, this means that a heavyweight protocol such as Radius or Diameter is going to be used over the air, which does not make up for good use of scarce radio resources.

THE INVENTION

It should be understood that although the invention will mainly be described with reference to access control of nodes in a NEMO-based Mobile Network, the inventive mechanisms, including filtering and control mechanisms, can be applied to mobile networks in general as well as in other communication contexts. For example, the invention is applicable in any mobile network architecture involving a mobile router located in the mobile network, and a counterpart node in the network side which anchors the mobility aspects of the mobile network. Other examples than NEMO-based mobile networks include HIP-based (Host Identity Protocol) mobile networks and mobile networks based on prefix scope binding update.

In the following, exemplary embodiments of the invention will be described, including preferred features as well as optional features.

(1) Access control enforcement points (EP's) are located at both the Mobile Router and Mobile Router Home Agent.

There is conceivable benefit with locating the EP's both at the Mobile Router and the Mobile Router Home Agent (MRHA) since unauthorized packets, both uplink and downlink, do not have to cross the air interface before being filtered away by the EP's. This prevents waste of precious radio resources. The EP located at the Mobile Router, called EP_MR for ease of description, monitors the uplink packets before the NEMO bidirectional tunnel, while the EP located

at the Mobile Router Home Agent, called EP_MRHA for ease of description, monitors the downlink packets before the NEMO bi-directional tunnel.

Fig. 1 illustrates authentication and/or authorization of nodes in NEMO-based Mobile Networks (PANA, PAA-EP, and EP-EP protocols traverse inside the NEMO bi-directional tunnel).

Preferably, the filtering mechanism involves checking the IP/transport layer headers of IP packets that traverse the access control points, also referred to as enforcement points EP, to and from the node in the mobile network. As mentioned, an idea according to the invention is to locate an EP at the mobile router to monitor/check/filter uplink packets, and another EP at the network side anchor node to monitor/filter/check downlink packets. For example, the filters are "activated" (or provisioned) in the EP after successful authentiction and authorization of the node in the mobile network. This process of activation involves provisioning of information, e.g. using SNMP. The provisioning may be carried out over the PAA-EP interface or possibly the EP-EP interface in the hierarchical structure model described below.

For comparison, reference [2] assumes that the access control function (enforcement point) is located in the Network Access Server, which is the Mobile Router for this case, and does not prevent unauthorized downlink packets from crossing the air interface before being filtered away at the Mobile Router.

(2) Two exemplary concepts and structures involving EP_MRHA and EP_MR are given below:

(i) A flat structure where both EP_MRHA and EP_MR receive the same provisioning information from the same access control list source. Fig. 2 illustrates an exemplary flat structure (no EP-EP interface).

(ii) A hierarchical structure where the EP_MRHA receives the provisioning information from the access control list source and thereafter the EP_MRHA forwards to the EP_MR under its control only the information pertinent to the uplink direction, i.e. an EP-EP interface. There can be a 1-to-n relationship between EP_MRHA and EP_MR. Fig. 3 illustrates an exemplary hierarchical structure (with EP-EP interface).

The advantage of concept (i) is the simplicity of implementation. Concept (i) does not require any EP-EP interface.

The advantage of concept (ii) is that extraneous provisioning information such as those pertaining to downlink filtering need not be sent over the air interface towards the EP_MR, and also, e.g., the EP_MR may not need to collect accounting information which can be collected at the EP_MRHA anyhow. This prevents waste of radio resources especially for cases where there is frequent movement of nodes in and out of the mobile network.

The provisioning information normally includes the resulting authorization information and among other things may involve the filters (i.e. the access control list) and restrictions to be used by the EP's, the accounting, and QoS markings that has to be carried out by the EP's.

Fig. 4 illustrates an example of the provisioning signaling flow for concept (i) with a flat structure.

Fig. 5 illustrates an example of the provisioning signaling flow for concept (ii) with a hierarchical structure (with EP-EP interface).

(3) For the case where the PANA (Protocol for carrying Authentication for Network Access) protocol [3] is used for access authentication and/or authorization of client nodes in NEMO-based Mobile Networks, the following configuration may be used:

a. PAC(s) (PANA Client(s)) is (are) located at the node(s).
b. PAA (PANA Authentication Agent) is located at the network where the MRHA resides, and is the access control list source that provisions the EP's as a result of client node access authentication

Locating the PAA at the network where the MRHA resides prevents a heavyweight AAA protocol such as Radius or Diameter from being used over the air interface.

Beyond the PAA towards and within the AAA infrastructure, suitable AAA carrier protocols (e.g., Diameter, Radius) may be used to carry the authentication and authorization information to and from the home network of the node.

(4) The PANA PAA-EP interface protocol [4] supports the additional requirement that it should be lightweight to accommodate possible air interface traversals.

Incidentally, reference [4] recommends the use of SNMP for the PAA-EP interface, which satisfies the lightweight requirement.

(5) The EP_MRHA-EP_MR (EP-EP) interface protocol for the hierarchical structure is defined to reuse the PANA PAA-EP interface protocol.

In effect, from the perspective of the EP_MR, the EP_MRHA is the access control list source, or PAA, that provisions the EP's as a result of client node access authentication. This simplifies the standardization/maintenance needed for the EP_MRHA-EP_MR interface protocol.

(6) For the case where SNMP is used for the PAA-EP interface, the SNMP MIBs are separated into convenient modules for uplink filtering, downlink filtering, IPSec uplink policy, IPSec downlink policy, accounting, etc., so as to facilitate simple implementation at the EP_MRHA, i.e., only the necessary MIB modules for uplink filtering and IPSec uplink policy can simply be forwarded to the EP_MR.

(7) The MRHA is selected/authorized as the local Home Agent for the node. This is for the case where the node is a Mobile IP mobile node, and a local Home Agent is allowed to be selected by the mobile node's home network operator and the network operator of the MRHA (e.g., via some inter-operator agreement).

Selecting the MRHA as the mobile node's local Home Agent where possible provides the possibility for route optimization as packets bound for the mobile node will have to traverse only one Home Agent instead of two.

The embodiments described above are merely given as examples, and it should be understood that the present invention is not limited thereto. Further modifications, changes and improvements which retain the basic underlying principles disclosed herein are within the scope of the invention.

REFERENCES

[1] Network Mobility (NEMO) Basic Support Protocol, Vijay Devarapalli, Ryuji Wakikawa, Alexandru Petrescu, Pascal Thubert, December 2003, <draft-ietf-nemo-basic-support-02.txt>.

[2] Protocol for Carrying Authentication for Network Access (PANA), D. Forsberg, Y. Ohba, B. Patil, H. Tschofenig, A. Yegin, October 24, 2003, <draft-ietf-pana-pana-02.txt>.

[3] PANA PAA-EP Protocol Considerations, Yacine El Mghazli, October 2003, <draft-yacine-pana-paa2ep-prot-eval-00.txt>.

[4] Usage Scenario and Requirements for AAA in Network Mobility Support, C.W. Ng, T. Tanaka, October 2002, <draft-ng-nemo-aaa-use-00.txt>.

ABBREVIATIONS

AAA – Authentication Authorization and Accounting
EP – Enforcement Point
EP_MR – Enforcement Point at Mobile Router
EP_MRHA – Enforcement Point at Mobile Router Home Agent
MR – Mobile Router
MRHA – Mobile Router Home Agent
NEMO – Network Mobility
PAA – PANA Authentication Agent
PAC – PANA Client
PANA – Protocol for carrying Authentication for Network Access
SNMP – Simple Network Management Protocol

1/5

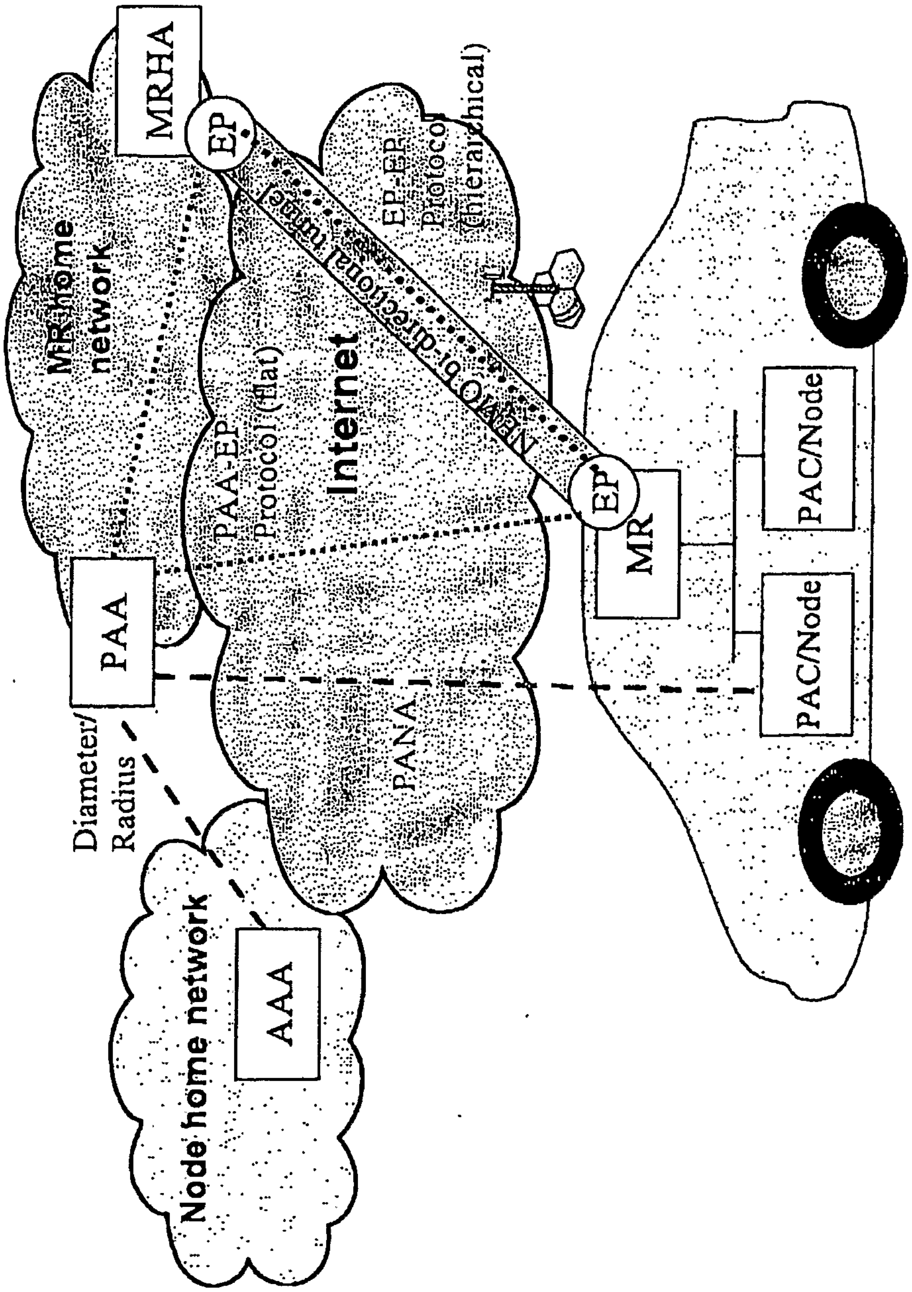


Fig. 1

BEST AVAILABLE COPY

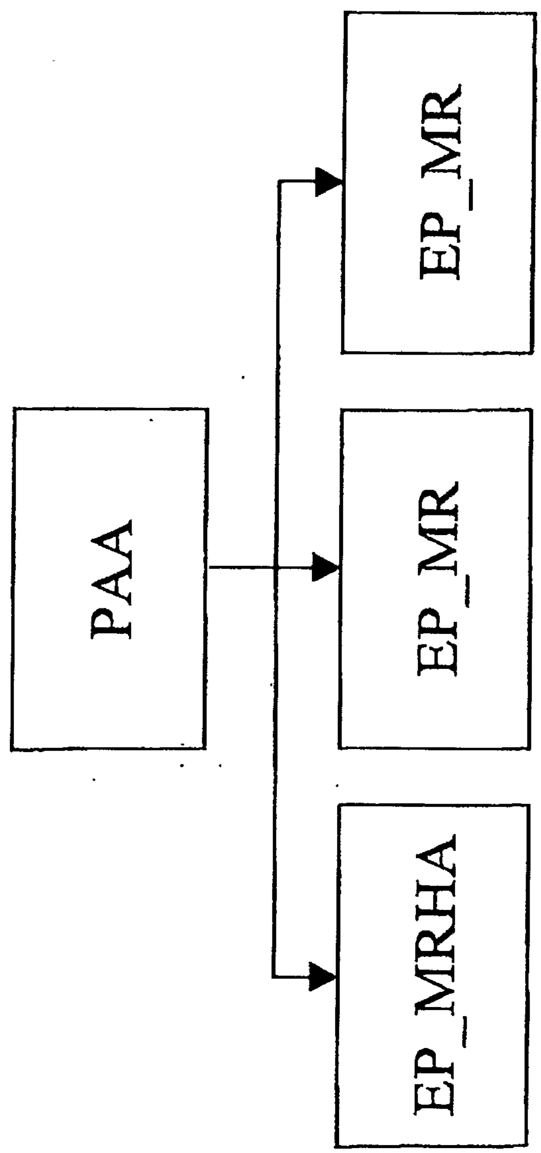


Fig. 2

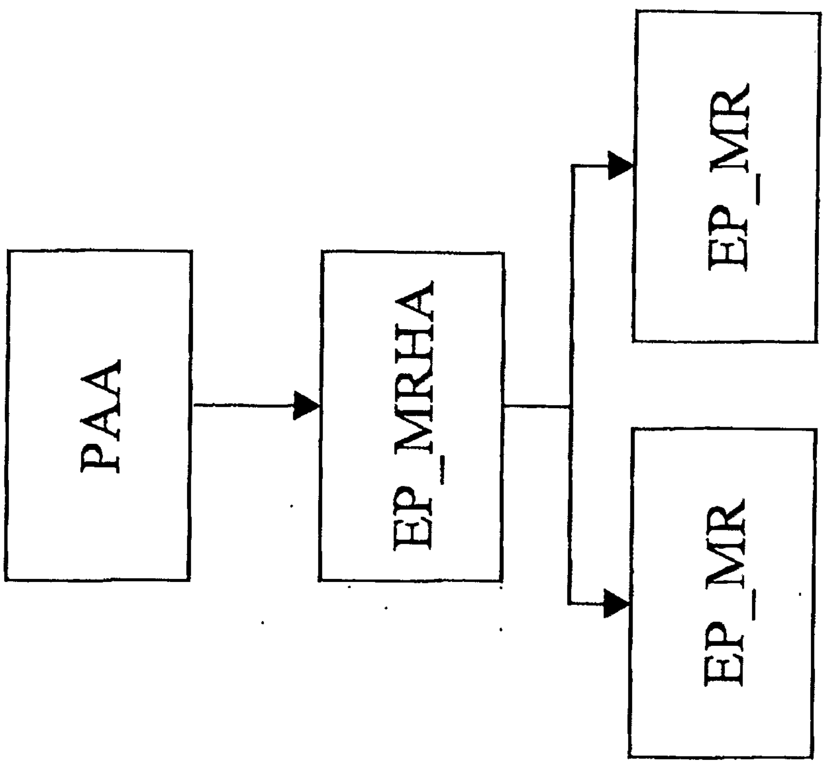


Fig. 3

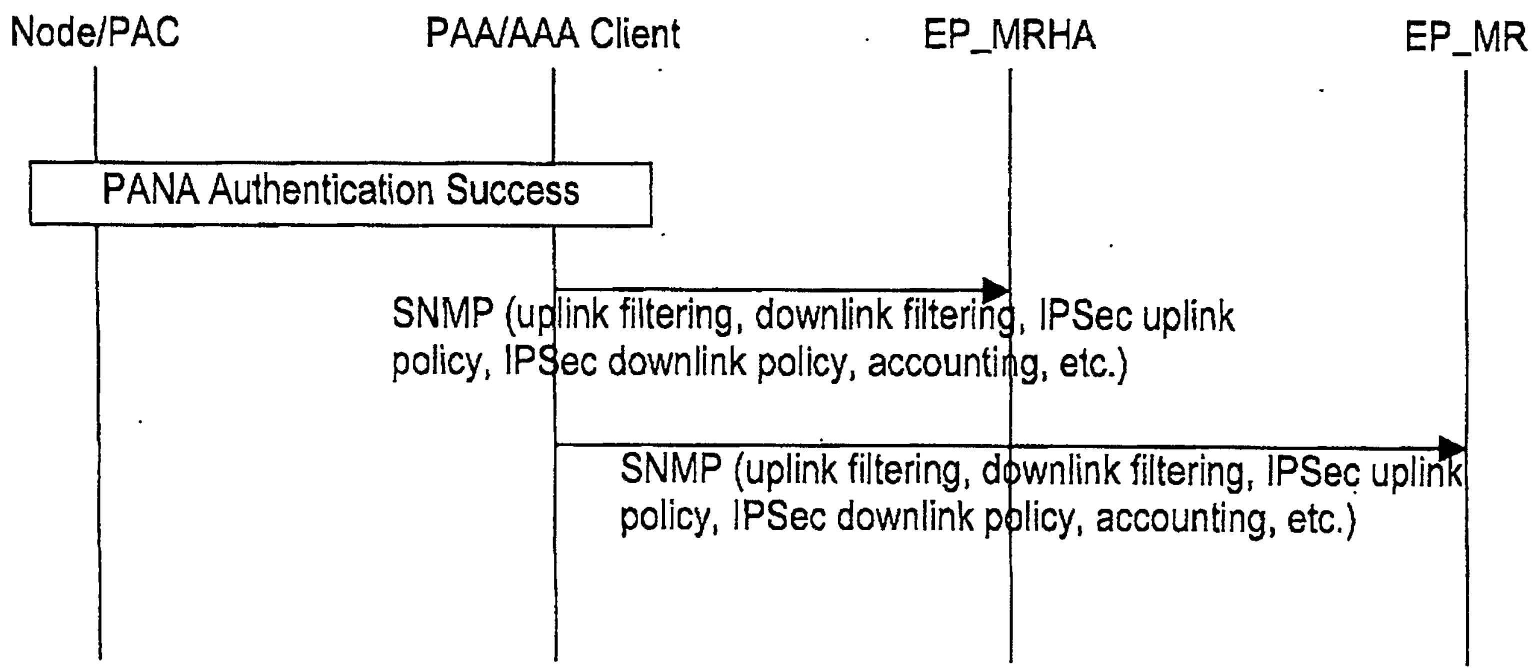
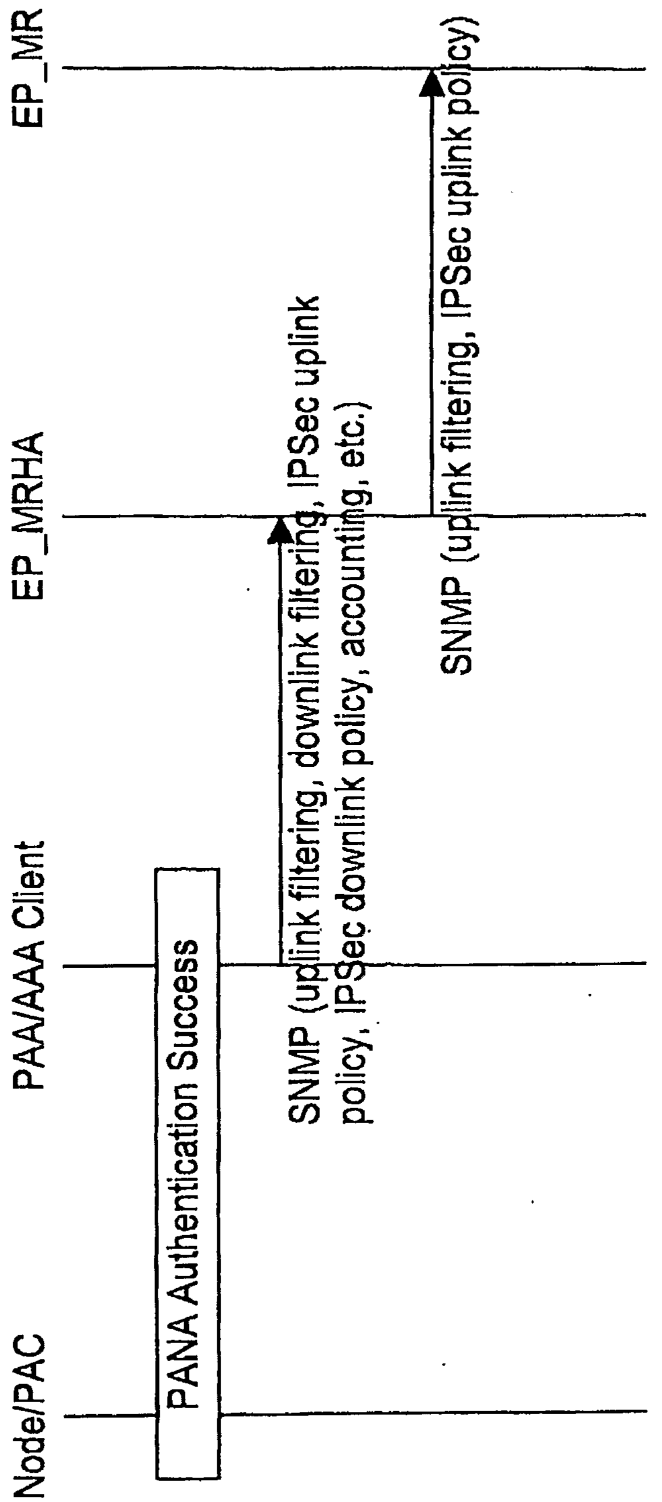

Node/PAC
PAA/AAA Client
EP_MRHA
EP_MR
PANA Authentication Success
SNMP (uplink filtering, downlink filtering, IPSec uplink policy, IPSec downlink policy, accounting, etc.)
SNMP (uplink filtering, downlink filtering, IPSec uplink policy, IPSec downlink policy, accounting, etc.)

Fig. 4



Node/PAC
PAA/AAA Client
EP_MRHA
EP_MR
PANA Authentication Success
SNMP (uplink filtering, downlink filtering, IPSec uplink policy, IPSec downlink policy, accounting, etc.)
SNMP (uplink filtering, IPSec uplink policy)

Fig. 5